Policies and Procedures
POLICY: Physical Safeguards
Policy #17
Effective Date: April 2, 2014

Purpose: The ILHIE Authority is committed to preventing unauthorized physical access to workstations that can access Electronic Protected Health Information while ensuring that Authorized Users have appropriate access. Appropriate physical safeguards for the ILHIE Authority and Participants shall be those required by HIPAA, these Policies and Procedures, the Data Sharing Agreement and other Applicable Law.

Policy: The ILHIE Authority and Participants shall implement appropriate physical safeguards to prevent the inappropriate request, use, or disclosure of Electronic Protected Health Information other than as permitted by HIPAA, these Policies and Procedures, the Data Sharing Agreement and other Applicable Law. The ILHIE Authority encourages Participants to meet the HIPAA addressable specifications, to the extent deemed appropriate. All Authorized Users who use workstations will take all reasonable precautions to protect the confidentiality, integrity, and availability of Electronic Protected Health Information. This Policy and Procedure shall address the ILHIE Authority's physical safeguards and shall apply to the ILHIE Authority Workforce, contractors, Subcontractors and agents.

1.0 Facility Access Controls. The ILHIE Authority and Participants shall each implement policies and procedures to limit physical access to their respective electronic Information Systems, as defined in 45 C.F.R §164.304, and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

1.1 The ILHIE Authority and, to the extent required under HIPAA, Participants shall establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

1.2 The ILHIE Authority and, to the extent required under HIPAA, Participants shall each implement policies and procedures to safeguard facilities and the equipment therein from unauthorized physical access, tampering and theft.

1.3 The ILHIE Authority and, to the extent required under HIPAA, Participants shall each implement procedures to control and validate a person's access to facilities based on that person's role or function, including visitor control, and control of access to software programs for testing and revisions.

1.4 The ILHIE Authority and, to the extent required under HIPAA, Participants shall each implement policies and procedures to document repairs and modifications to the physical components of facilities which are related to security (for example, hardware, walls, doors and locks).

2.0 **Workstation Use.** The ILHIE Authority and Participants shall each implement policies and procedures, for each specific workstation or class of workstation that can access Electronic Protected Health Information, that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of the specific workstation or class of workstations.

3.0 **Workstation Security.** The ILHIE Authority and Participants shall each implement physical safeguards for all workstations and other devices (including those accessed via secure, encrypted, remote access) that access Electronic Protected Health Information, to restrict access to Authorized Users.

3.1 Workstation security safeguards shall include password controls, including controls for physically unattended workstations, consistent with the User Authentication Policy (Policy #3).

4.0 **Device and Media Control.** The ILHIE Authority and Participants shall each implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain Electronic Protected Health Information into and out of a facility, and the movement of these items within the facility.

4.1 The ILHIE Authority and Participants shall each implement policies and procedures to address the final disposition of Electronic Protected Health Information, and/or the hardware or electronic media on which it is stored.

4.2 The ILHIE Authority and Participant shall each implement policies and procedures for removal of Electronic Protected Health Information from electronic media before the media are made available for re-use.

4.3 The ILHIE Authority and, to the extent required under HIPAA, Participants shall each maintain a record of the movement of hardware and electronic media and any person responsible therefore.

4.4 The ILHIE Authority and, to the extent required under HIPAA, Participants shall each create a retrievable, exact copy of Electronic Protected Health Information, when needed, before movement of equipment.

5.0 **Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

5.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Procedures:

The ILHIE Authority and, to the extent required under HIPAA, Participants will each comply with or implement the following procedures.

1.0 Information Systems and other electronic media containing Protected Health Information must be located and stored in secure environments that are protected by appropriate security barriers and entry controls.

2.0 Reasonable measures to prevent viewing Electronic Protected Health Information on workstations by unauthorized persons must be taken.

3.0 Regularly conduct a formal, documented process that ensures consistent control and protection of all electronic media and Information Systems containing Electronic Protected Health Information that is created, sent, received or destroyed.

4.0 Authorized Users who move electronic media or Information Systems containing Electronic Protected Health Information are responsible for the subsequent use of such items and must take all appropriate and reasonable actions to protect them against damage, theft and unauthorized access.

5.0 All Electronic Protected Health Information must be permanently removed from the hardware and electronic media on which the Electronic Protected Health Information is stored before the devices can be discarded or re-used.

6.0 Electronic Protected Health Information shall not be stored on removable media or portable workstation unless encrypted.

Associated Policies & References
45 C.F.R §164.310
Illinois Health Information Exchange System Security Plan (SSP)
User Authorization

Definitions
Authorized Users
Electronic Protected Health Information
HIPAA
ILHIE Authority
Information Systems
Participants
Subcontractors
Workforce